Making Security Measurable™

BUILDING SECURITY IN

SOFTWARE ASSURANCE

Information Exchange Using IODEF and RID

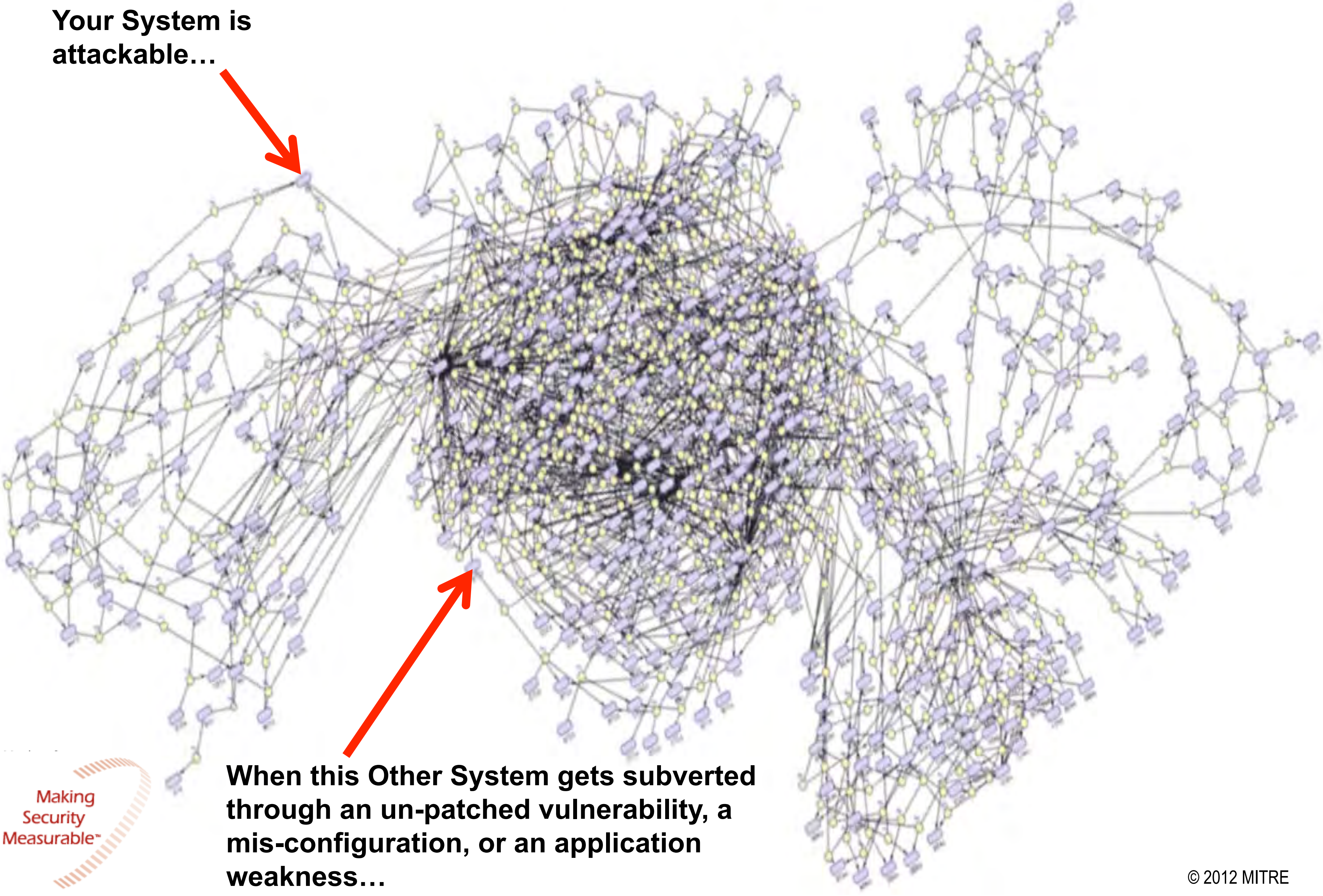
March 26, 2012

MITRE

Outline

- Coordinated Incident Response
  - **Problem Statements**
  - **Current State**
- Protocols and development
  - **Incident Object Description and Exchange Format**
  - **Real-time Inter-network Defense**
- Managed Incident Lightweight Exchange (MILE)

Today Everything's Connected – Like an Ecosystem

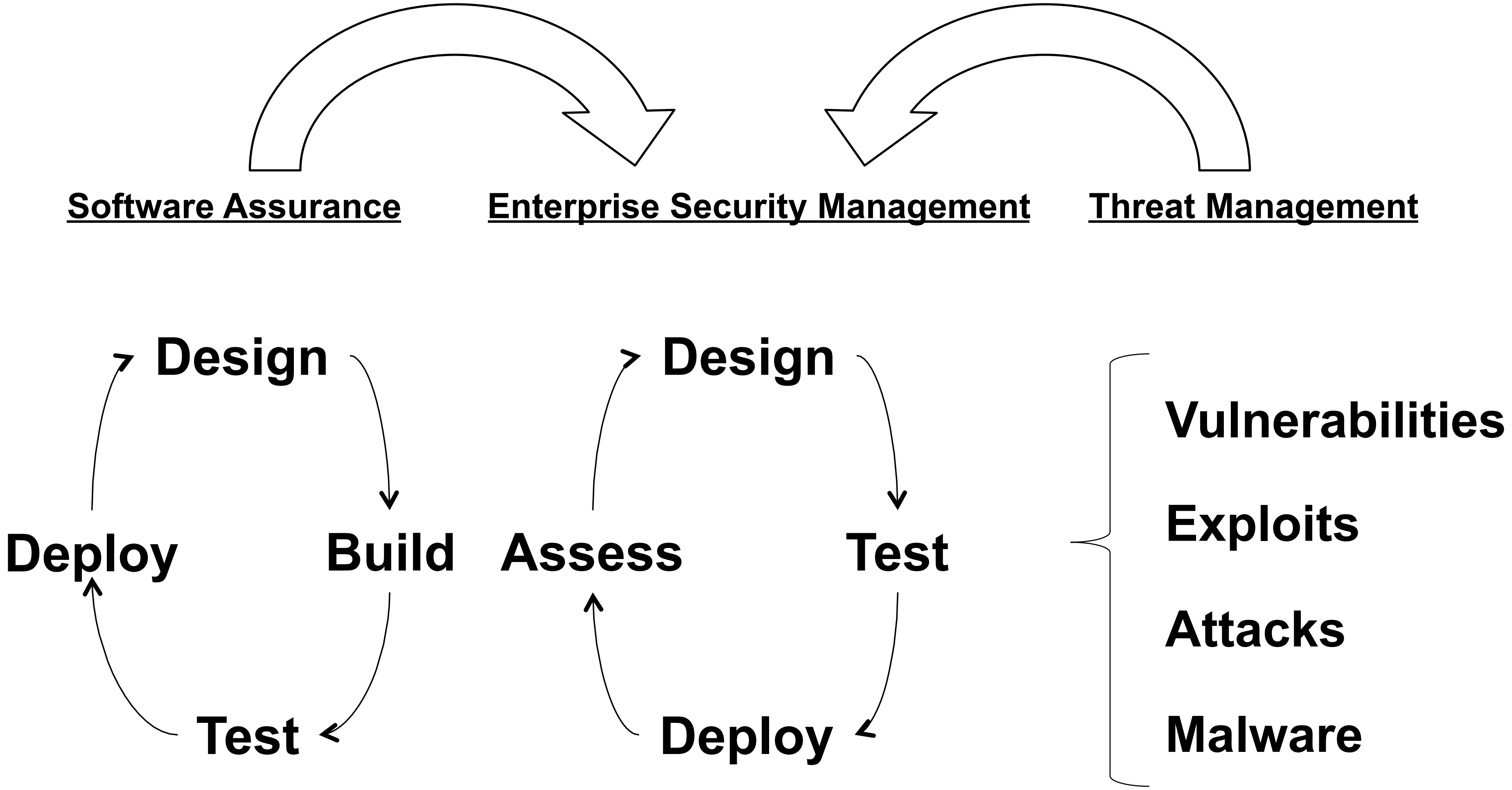


Your System is attackable…

When this Other System gets subverted through an un-patched vulnerability, a mis-configuration, or an application weakness…

Making Security Measurable™

Making Security Measurable (MSM)
“You Are Here”



Software Assurance

Enterprise Security Management

Threat Management

Design

Build

Test

Deploy

Design

Test

Deploy

Assess

Vulnerabilities

Exploits

Attacks

Malware

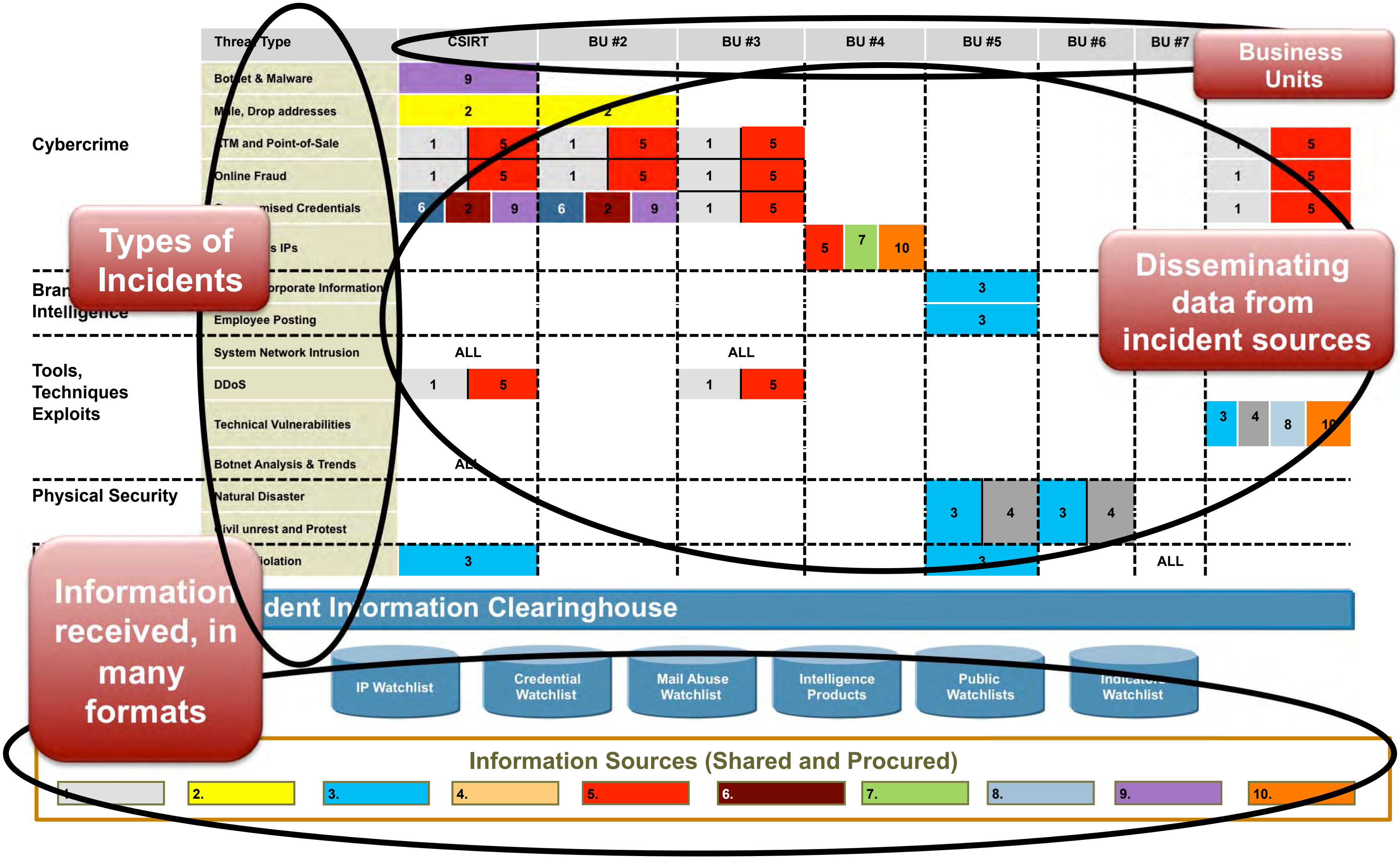
CWE, CAPEC, CWSS, CWRAF

CPE, CCE, OVAL, OCIL, XCCDF, AssetId, ARF

CVE, CWE, CAPEC, MAEC, CybOX, IODEF, RID, RID-T, CYBEX

© 2012 MITRE

Problem Statement 1:
Incident Information: Collect, Process, & Manage



	Threat Type	CSIRT	BU #2	BU #3	BU #4	BU #5	BU #6	BU #7	
Cybercrime	Botnet & Malware	9							
	Mule, Drop addresses	2	2						
	ATM and Point-of-Sale	1 5	1 5	1 5					1 5
	Online Fraud	1 5	1 5	1 5					1 5
	mised Credentials	6 2 9	6 2 9	1 5					1 5
	s IPs				5 7 10				
Bran Intelligence	orporate Information					3			
	Employee Posting					3			
Tools, Techniques Exploits	System Network Intrusion	ALL		ALL					
	DDoS	1 5		1 5					
	Technical Vulnerabilities								3 4 8 10
	Botnet Analysis & Trends	ALL							
Physical Security	Natural Disaster					3 4	3 4		
	ivil unrest and Protest								
	iolation	3				3		ALL	

Business Units

Types of Incidents

Disseminating data from incident sources

Information received, in many formats

dent Information Clearinghouse

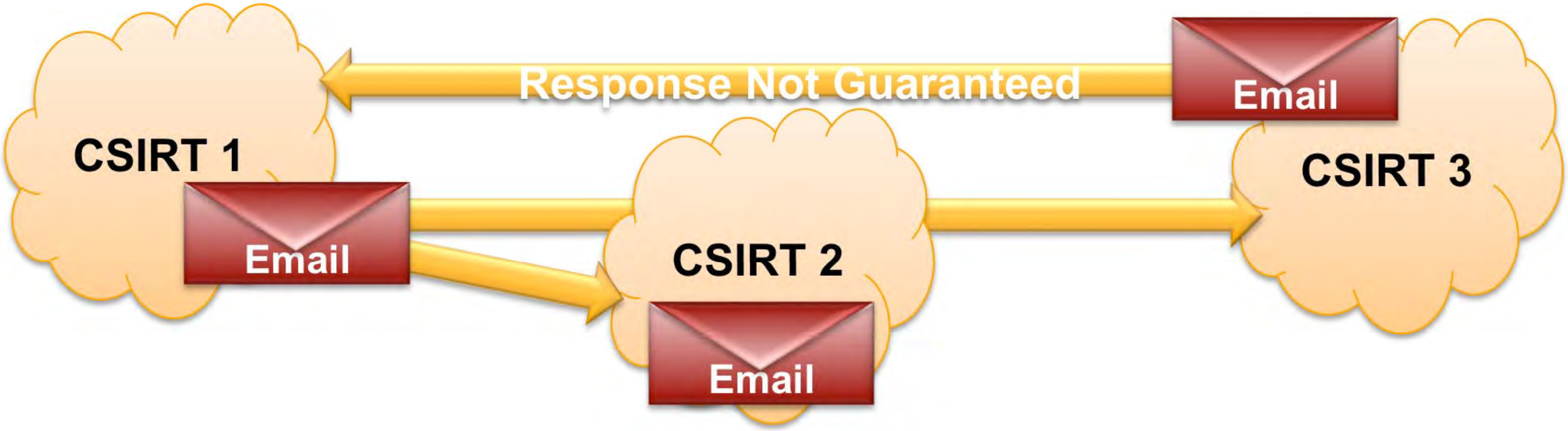
Information Sources (Shared and Procured)

1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

© 2012 EMC, presented with permission by MITRE,

Problem Statement 2:
Secure Exchange of Incident Information

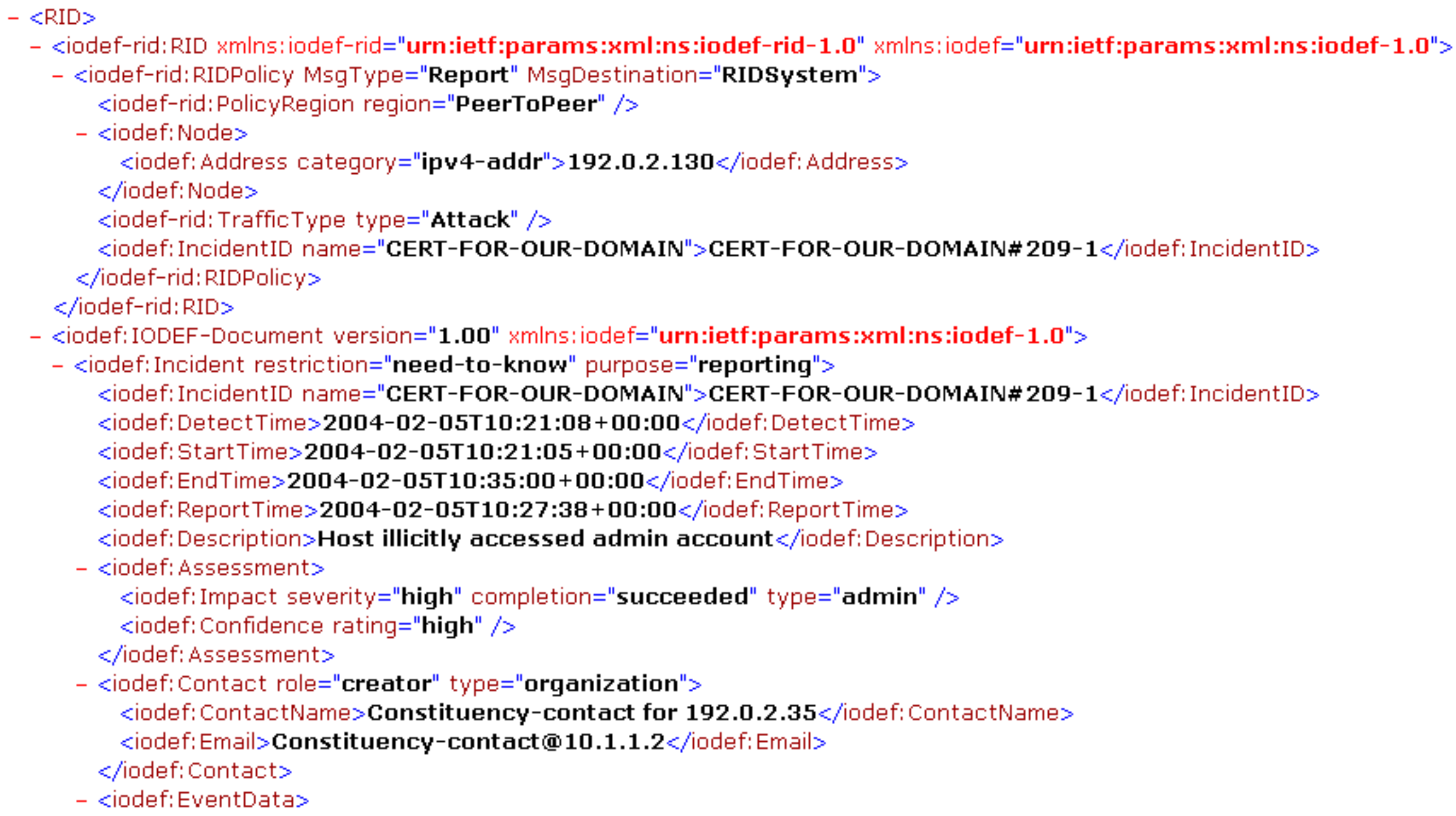
Communication Difficult via Email and Phone Calls



- Necessary to share sensitive information in order to mitigate or stop an incident
- Difficult to know the status of an incident or what was done to resolve it
- Handled through phone calls and email, even when mail systems may be the target of attacks
- Finding the right contacts is difficult to track down and respond to an incident
- If information is passed through multiple CSIRTs, no way to know where a request truly originated
- Incident may sit in an individual's inbox for a long period of time, response not guaranteed
- No established Agreements between CSIRTs or CSIRTs and their clients for handling of incidents

Problem Statement 3:
XML is Ugly

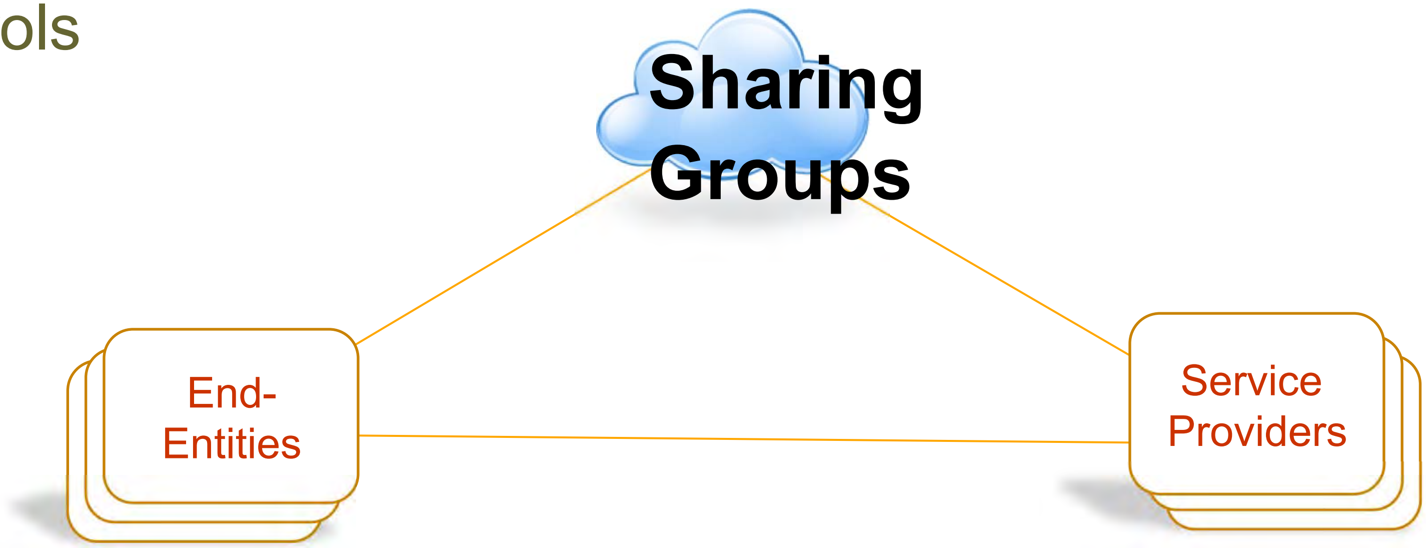
Incident Responders should have XML and Security Hidden in Secure Exchanges



```
- <RID>
  - <iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0" xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
    - <iodef-rid:RIDPolicy MsgType="Report" MsgDestination="RIDSystem">
        <iodef-rid:PolicyRegion region="PeerToPeer" />
      - <iodef:Node>
          <iodef:Address category="ipv4-addr">192.0.2.130</iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType type="Attack" />
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">CERT-FOR-OUR-DOMAIN#209-1</iodef:IncidentID>
      </iodef-rid:RIDPolicy>
    </iodef-rid:RID>
  - <iodef:IODEF-Document version="1.00" xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
    - <iodef:Incident restriction="need-to-know" purpose="reporting">
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">CERT-FOR-OUR-DOMAIN#209-1</iodef:IncidentID>
        <iodef:DetectTime>2004-02-05T10:21:08+00:00</iodef:DetectTime>
        <iodef:StartTime>2004-02-05T10:21:05+00:00</iodef:StartTime>
        <iodef:EndTime>2004-02-05T10:35:00+00:00</iodef:EndTime>
        <iodef:ReportTime>2004-02-05T10:27:38+00:00</iodef:ReportTime>
        <iodef:Description>Host illicitly accessed admin account</iodef:Description>
      - <iodef:Assessment>
          <iodef:Impact severity="high" completion="succeeded" type="admin" />
          <iodef:Confidence rating="high" />
        </iodef:Assessment>
      - <iodef:Contact role="creator" type="organization">
          <iodef:ContactName>Constituency-contact for 192.0.2.35</iodef:ContactName>
          <iodef:Email>Constituency-contact@10.1.1.2</iodef:Email>
        </iodef:Contact>
      - <iodef:EventData>
```

Problem Statement 4:
Trust Relationships to Support Exchange

Trusted information sharing with policy mapped to security controls



- RID supports the secure exchange of incident information for sharing purposes and incident handling
- Method needed to easily establish trust between entities
  - **Encryption**
  - **Authentication**
  - **Integrity**
  - **Non-repudiation**
- CloudSIRT looking to use IODEF/RID for increased visibility in the cloud between providers and also to tenants

Outline

- Coordinated Incident Response
  - **Problem Statements**
  - **Current State**
- Protocols and development
  - **Incident Object Description and Exchange Format**
  - **Real-time Inter-network Defense**
- Managed Incident Lightweight Exchange (MILE)

Incident Object Description and Exchange Format (IODEF)

Background

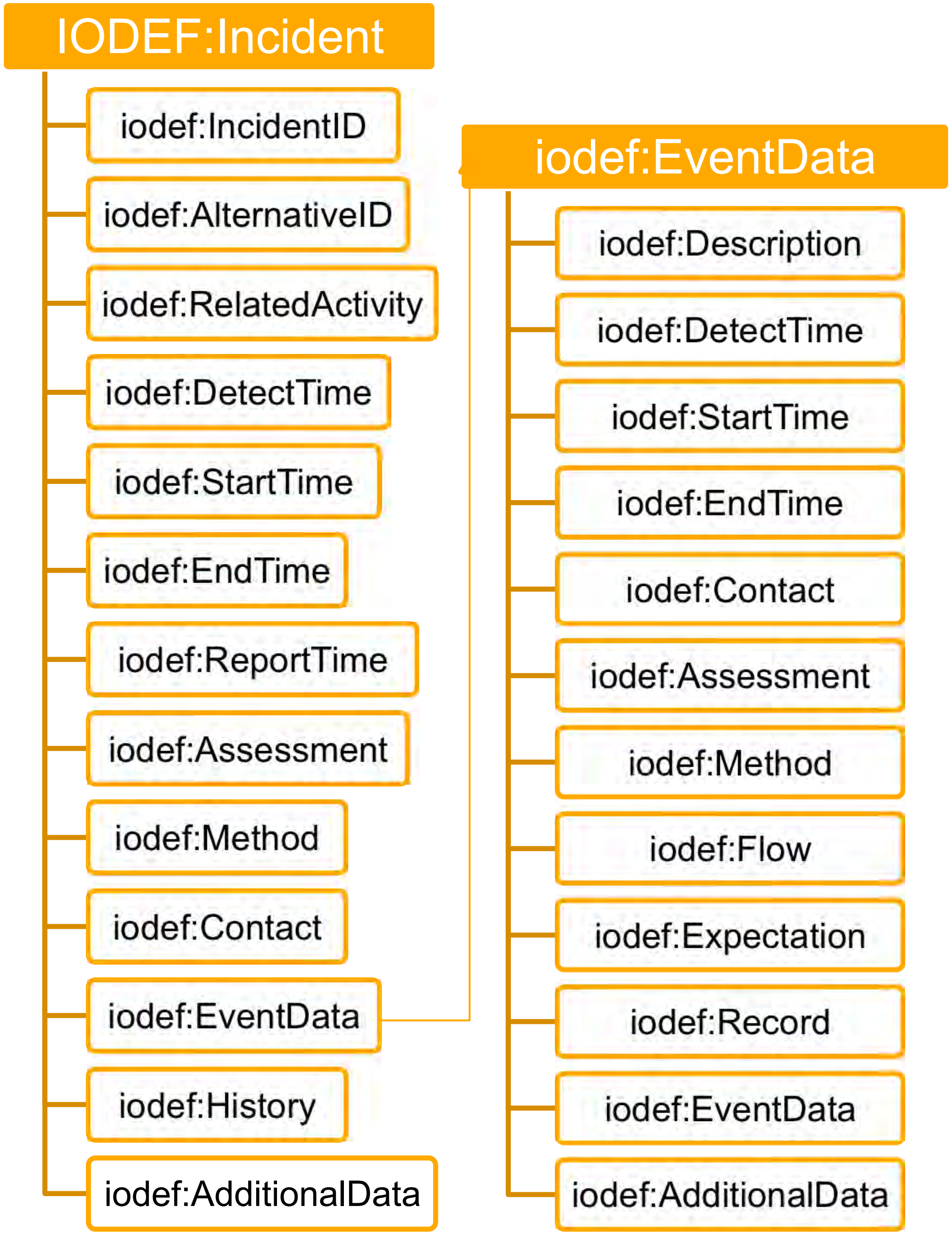
- Internet Engineering Task Force (IETF) Standard: RFC5070
- Provides a standard format to describe a security incident
- Effort led by the CERT Coordination Center (CERT/CC) out of Carnegie Mellon University
- Computer Security Incident Response Teams (CSIRTs) globally contributed to the development and evaluation of the Extensible Markup Language (XML) schema

Assumptions

- Incidents are not IDS alarms
  - **"Incidents are composed of events"**
- Agnostic to specific incident taxonomies
  - **"Your definition/threshold of an incident may be different than mine"**
- Incidents are numbered and there is state kept about them
  - **"Organizations assign incident IDs and have ticketing/handling/correlation systems that process them"**
- Merely a wire format
  - **"Sharing is different than storage and archiving"**
- Incomplete information
  - **"You may require more complete information than I need, can get, or have right now"**

IODEF Data Model

- CSIRT Operations
  - **Incident identifiers**
  - **Contact Information**
- Internationalization
  - **Various Encodings**
  - **Translations**
- Data handling labels
  - **Sensitivity**
  - **Confidence**
- Extensibility of attributes and adding new elements
- Timing information
- Enumeration of hosts or networks
  - **e.g., IP addresses, ports, protocols, applications, etc.**
- History and requested action
- Exploit and vulnerability references
- Impact expressed technically, financially, or by time
- Forensics information



Real-time Inter-network Defense (RID)

RID Purpose and Security

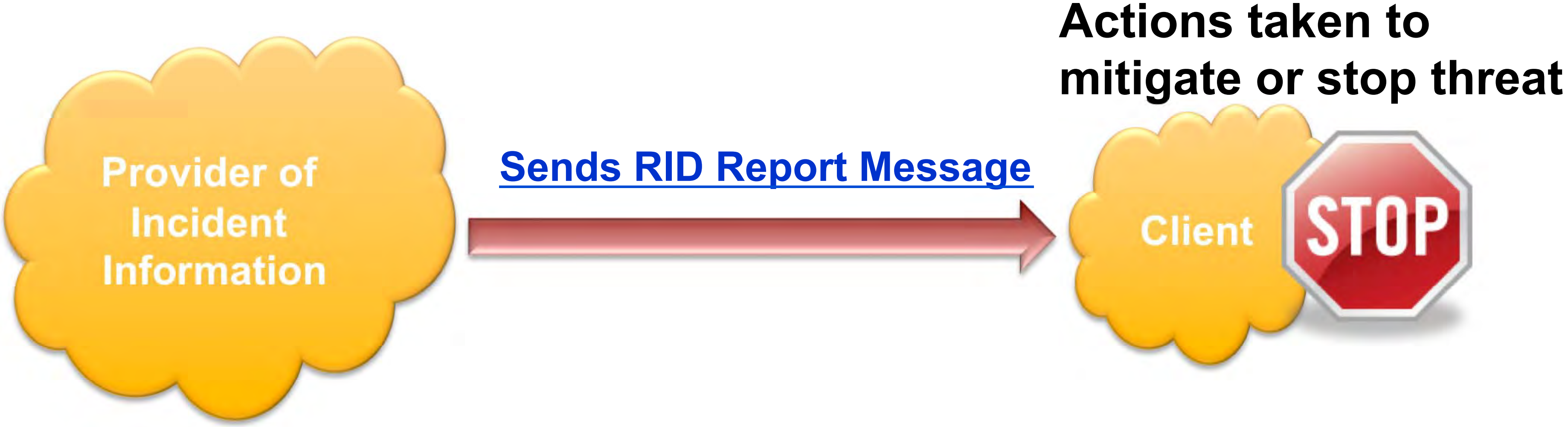
- Goal: Exchange or share incident information
  - **Facilitate secure communication of incident information between providers, entities, regions, or nations**
  - **Enable tracking of incidents as investigations evolve**
  - **Trace incidents to the source**
  - **Stop or mitigate the effects of an attack**
  - **Integrate with existing and future infrastructure components**
- Security and Privacy Considerations:
  - **Session and stored encryption**
    - XML digital signatures and encryption
    - TLS used in transport
  - **Authentication for single and multi-hop scenarios**
  - **Consortiums to establish trust relationships**
  - **Regional and international security and language barriers addressed via IETF Internationalization**
  - **Privacy: Data restriction markings, ability to optionally provide full data, anonymize data, or encrypt based on markers**

RID Message Types

- Request
  - **Investigation**
  - **Trace**
- Acknowledgement
- Result
- Report
- Query

Sharing Incident Information

IODEF, extensions to IODEF, and RID

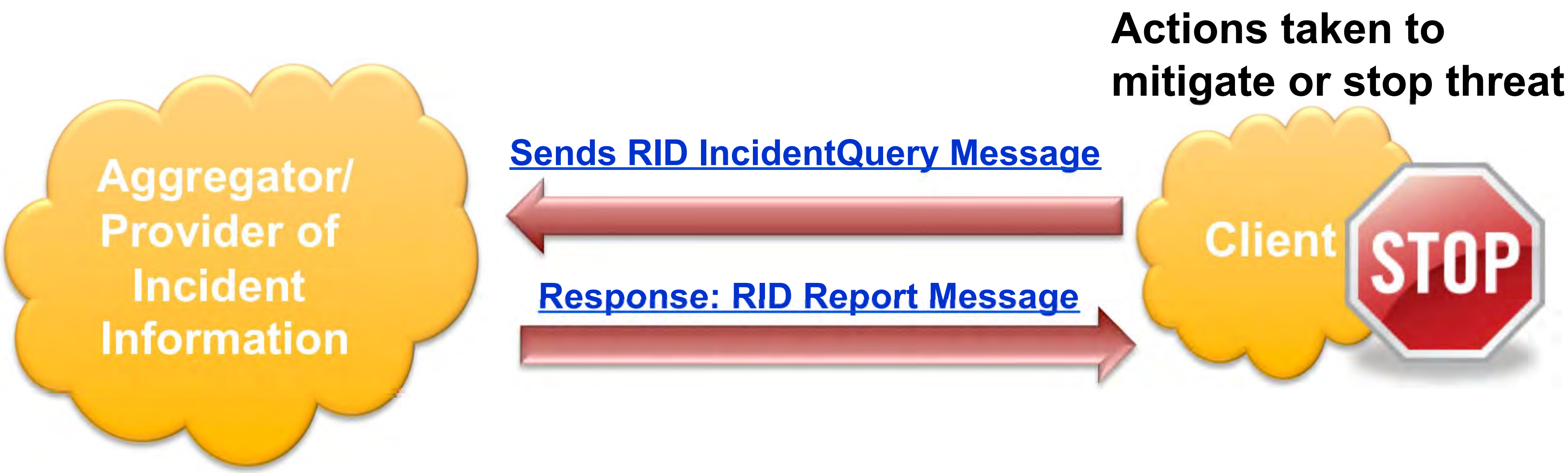

Actions taken to mitigate or stop threat
Provider of Incident Information
Sends RID Report Message
Client
STOP

- IODEF formatted incident report
  - **May be anonymized**
  - **May be sent out to all clients or applicable client(s)**
- Security, Privacy and policy provided via RID and transport

© 2012 EMC, presented with permission by MITRE,

Query Incident Information

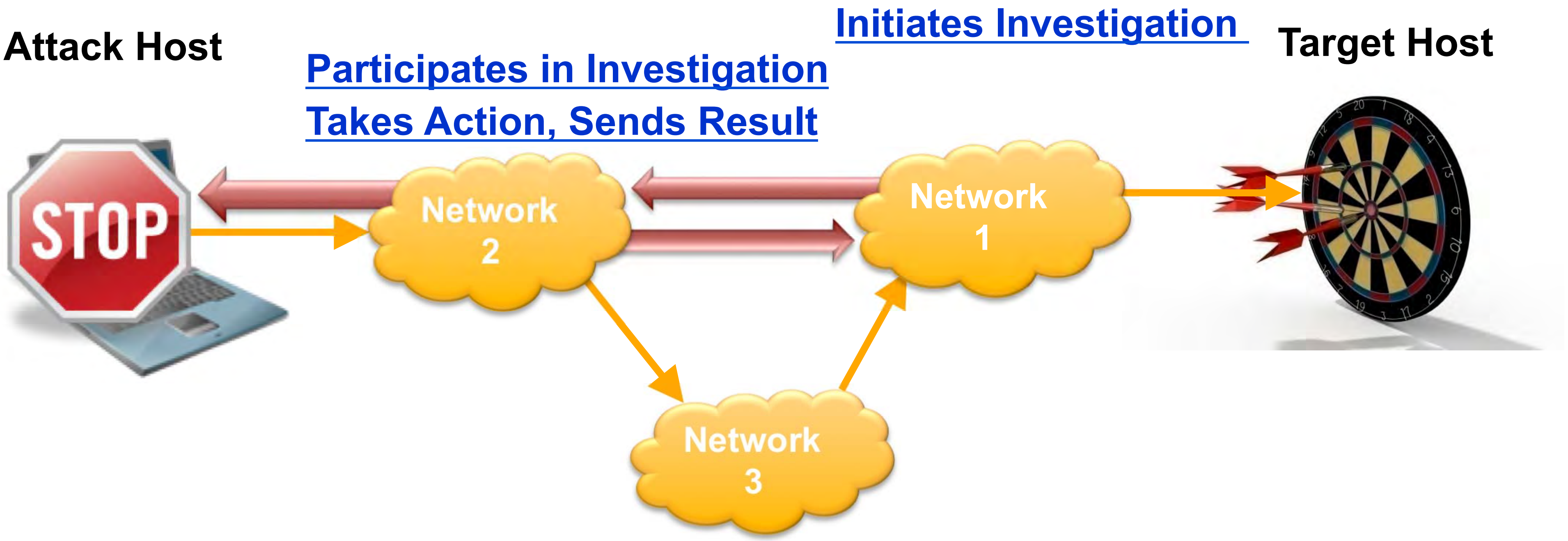
RID Exchange to Query Incident Information


Actions taken to mitigate or stop threat
Aggregator/ Provider of Incident Information
Sends RID IncidentQuery Message
Response: RID Report Message
Client
STOP

- Client may be interested to know if others are seeing a specific type of incident or attack patterns
- Client sends request to Provider of Incident information
- RID Report message with IODEF document sent in response

RID: Investigation/TraceRequest Example

Investigation results in direct communication with source CSIRT



Attack Host

Participates in Investigation

Takes Action, Sends Result

Initiates Investigation

Target Host

Participates in TraceRequest

Investigation Only

Outline

- Coordinated Incident Response
  - **Problem Statements**
  - **Current State**
- Protocols and development
  - **Incident Object Description and Exchange Format**
  - **Real-time Inter-network Defense**
- Next Steps

Incident Information Exchanges

- National Information Exchange Model (NIEM)
- Anti-Phishing Working Group (APWG)
- Research and Education Network – Information Sharing and Analysis Center (REN-ISAC)
- Japan Computer Emergency Response Team (JP-CERT)
- Cyber Security Information Exchange Tool (CYBIET) Project
- Cloud Security Alliance CloudSIRT
- Industry, led by financial sector, asks DHS to share incident information
- DoD: NIST business use case adopted by Unified Cross Domain Management Office (UCDMO) (IODEF and RID)
- NATO is reviewing RID and IODEF in their Cyber Defense Data eXchange and Collaboration Infrastructure (CDXI)

Outline

- Coordinated Incident Response
  - **Problem Statements**
  - **Current State**
- Protocols and development
  - **Incident Object Description and Exchange Format**
  - **Real-time Inter-network Defense**
- Managed Incident Lightweight Exchange (MILE)

Managed Incident Lightweight Exchange (MILE)

IETF Working Group extending base specifications

- MILE is an active working group improving the existing standards and building extensions to fit evolving use cases
- RID and the Transport of RID over HTTP/TLS have been updated
- IODEF will have a guidance document starting soon
- Extensions currently include:
  - **Incorporating other XML schemas as appropriate in the Structured Cybersecurity Information extension**
  - **Data Markers to enable decisions based on markers**
  - **Forensics**
  - **Mail abuse**
- A lightweight version of IODEF may be developed

Summary

MILE: IODEF, RID, and new Extensions

- IODEF and RID are IETF standards with additional standardization activity in progress
  - **Need to implement standardized incident formats has become more prevalent in the enterprise**
    - CSIRTs at the enterprise level increasing, driven by business requirements and increases in Fraud
    - Easier to aggregate, process, and disseminate incident information within the organization
    - Requires ability to correlate incidents to system configuration & vulnerabilities (SCAP + IODEF + RID)
  - **New extension formats are required to standardize exchanges for specific incident types and data classification requirements**
- Increase in severity of incidents and outsourcing (Cloud) is driving the need for automation in incident response

Contact Info

Robert A. Martin
Principal Engineer
Making Security Measurable
ramartin@mitre.org

Kathleen M. Moriarty
EMC Office of the CTO
kathleen.moriarty@emc.com